CLAIMS

1. A method for processing data packets in a computer network, comprising:

configuring a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receiving a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determining if there is a match between the data packet and one or more of the packet policies, each packet policy authorizing matching data packets to use the computer network;

if there is a matching packet policy authorizing the data packet, routing the data packet using a Layer 2-3 switch; and

if there is no matching packet policy authorizing the data packet, blocking the data packet.

2. The method of claim 1, wherein the user defined packet policies include timed packet policies, the timed packet policies being active during specified date or time intervals, and determining if there is at least one matching packet policy comprises:

determining if there is a currently active timed matching policy.

3. The method of claim 1, wherein the user defined packet policies authorize data packets being transmitted or received by authorized users, applications, physical ports, application ports, IP addresses, or MAC addresses.

4. The method of claim 1, wherein blocking the data packet comprises:

discarding the data packet, logging the data packet, or forwarding the data packet to a multilayer switch application for processing.

5. A method for processing data packets in a computer network, comprising:

configuring a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receiving a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determining if there is a match between the data packet and one or more packet policies that specify a second packet policy to be applied to the matching data packets, the second packet policy having one or more policy action fields; and

if there is a matching packet policy specifying a second packet policy, processing the data packet based on the policy action fields of the second packet policy.

6. The method of claim 5, wherein the matching packet policy specifies the application of a preexisting second packet policy, and processing the data packet comprises:

identifying the preexisting second packet policy specified by the matching packet policy; and

processing the data packet based on the policy action fields of the preexisting second packet policy.

7. The method of claim 5, wherein the matching packet policy specifies the application of a dynamically created second packet policy, and processing the data packet comprises:

creating the second packet policy specified by the matching packet policy; and

processing the data packet based on the policy action fields of the created second packet policy.

8. The method of claim 5, wherein processing the data packet comprises:

routing the data packet using a Layer 2-3 switch.

9. A method for processing data packets in a computer network, comprising:

configuring a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receiving a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determining if there is a match between the data packet and one or more packet policies, that assign a quality of service (QoS) metric to matching data packets;

if there is a matching packet policy assigning a QoS metric to the data packet, determining a priority for the data packet based on the assigned QoS metric; and

routing the data packet using a Layer 2-3 switch based on the priority.

10. The method of claim 9, wherein the QoS metric specifies prioritization, bandwidth allocation, minimum bandwidth allocation, maximum bandwidth allocation, or network access permission for the data packet.

11. The method of claim 9, wherein assigning a QoS metric includes assigning a QoS metric based on application, application type, application port, physical port, elapsed time, time of day, day of week, date or time interval.

12. The method of claim 9, wherein assigning a QoS metric includes assigning a QoS metric for individual users, workgroups, VLAN, subnets, networks, IP addresses, IP address range, MAC addresses, and MAC address range.

13. A method for processing data packets in a computer network, comprising:

configuring a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receiving a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model, the data packet being part of a network flow representing access to a specific website;

determining if there is a match between the data packet and one or more of the packet policies, the matching packet policies authorizing access to the specific website;

if there is a matching packet policy authorizing access to the specific website, routing the data packet using a Layer 2-3 switch; and

if there is no matching packet policy authorizing access to the specific website, blocking the data packet.

14. The method of claim 13, wherein the user defined packet policies include timed packet policies, the timed packet policies being active during specified date or time intervals, and determining if there is at least one matching packet policy comprises:

determining if there is a currently active timed matching policy authorizing access to the specific website.

15. The method of claim 13, wherein the user defined packet policies authorize access to specific websites by authorized users, applications, physical ports, application ports, IP addresses, or MAC addresses.

16. The method of claim 13, wherein blocking the data packet comprises:

discarding the data packet, logging the data packet, or forwarding the data packet to a multilayer switch application for processing.

17. A method for processing data packets in a computer network, comprising:

configuring a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receiving a data packet at a particular port of the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determining if there is a match between the data packet and one or more of the packet policies, each packet policy blocking matching data packets received at the particular port from utilizing the computer network;

if there is a matching packet policy blocking the data packet, blocking the data packet; and

if there is no matching packet policy blocking the data packet, processing the data packet.

18. The method of claim 17, wherein the user defined packet policies block data packets received at the particular port, for data packets having a subnet address, a range of subnet addresses, a host address, or a range of host addresses.

19. A method for processing data packets in a computer network, comprising:

configuring a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receiving a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determining if there is a match between the data packet and one or more of the packet policies, each packet policy specifying that surveillance is to performed on the data packet;

if there is a matching packet policy specifying surveillance, mirroring the data packet to a specified location; and

processing the data packet using the multilayer switch.

20. The method of claim 19, wherein processing the data packet comprises:

routing the data packet using a Layer 2-3 switch.

21. A computer program product tangibly embodied in a computer readable medium, the computer program product comprising instructions operable to cause data processing equipment to:

configure a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receive a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determine if there is a match between the data packet and one or more of the packet policies, each packet policy authorizing matching data packets to use the computer network;

if there is a matching packet policy authorizing the data packet, route the data packet using a Layer 2-3 switch; and

if there is no matching packet policy authorizing the data packet, block the data packet.

22. The computer program product of claim 21, wherein the user defined packet policies include timed packet policies, the timed packet policies being active during specified date or time intervals, and the instructions for determining if there is at least one matching packet policy cause the data processing equipment to:

determine if there is a currently active timed matching policy.

23. The computer program product of claim 21, wherein the user defined packet policies authorize data packets being transmitted or received by authorized users, applications, physical ports, application ports, IP addresses, or MAC addresses.

24. The computer program product of claim 21, wherein the instructions for blocking the data packet cause the data processing equipment to:

discard the data packet, log the data packet, or forward the data packet to a multilayer switch application for processing.

25. A computer program product tangibly embodied in a computer readable medium, the computer program product comprising instructions operable to cause data processing equipment to:

configure a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receive a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determine if there is a match between the data packet and one or more packet policies that specify a second packet policy to be applied to the matching data packets, the second packet policy having one or more policy action fields; and

if there is a matching packet policy specifying a second packet policy, process the data packet based on the policy action fields of the second packet policy.

26. The computer program product of claim 25, wherein the matching packet policy specifies the application of a preexisting second packet policy, and the instructions for processing the data packet cause the data processing equipment to:

identify the preexisting second packet policy specified by the matching packet policy; and

process the data packet based on the policy action fields of the preexisting second packet policy.

27. The computer program product of claim 25, wherein the matching packet policy specifies the application of a dynamically created second packet policy, and the instructions for processing the data packet cause the data processing equipment to:

create the second packet policy specified by the matching packet policy; and

process the data packet based on the policy action fields of the created second packet policy.

28. The computer program product of claim 25, wherein the instructions for processing the data packet cause the data processing equipment to:

routing the data packet using a Layer 2-3 switch.

29. A computer program product tangibly embodied in a computer readable medium, the computer program product comprising instructions operable to cause data processing equipment to:

configure a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receive a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determine if there is a match between the data packet and one or more packet policies, that assign a quality of service (QoS) metric to matching data packets;

if there is a matching packet policy assigning a QoS metric to the data packet, determine a priority for the data packet based on the assigned QoS metric; and

route the data packet using a Layer 2-3 switch based on the priority.

30. The computer program product of claim 29, wherein the QoS metric specifies prioritization, bandwidth allocation, minimum bandwidth allocation, maximum bandwidth allocation, or network access permission for the data packet.

31. The computer program product of claim 29, wherein assigning a QoS metric includes assigning a QoS metric based on application, application type, application port, physical port, elapsed time, time of day, day of week, date or time interval.

32. The method of claim 9, wherein assigning a QoS metric includes assigning a QoS metric for individual users, workgroups, VLAN, subnets, networks, IP addresses, IP address range, MAC addresses, and MAC address range.

33. A computer program product tangibly embodied in a computer readable medium, the computer program product comprising instructions operable to cause data processing equipment to:

configure a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receive a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model, the data packet being part of a network flow representing access to a specific website;

determine if there is a match between the data packet and one or more of the packet policies, the matching packet policies authorizing access to the specific website;

if there is a matching packet policy authorizing access to the specific website, route the data packet using a Layer 2-3 switch; and

if there is no matching packet policy authorizing access to the specific website, block the data packet.

34. The computer program product of claim 33, wherein the user defined packet policies include timed packet policies, the timed packet policies being active during specified date or time intervals, and the instructions for determining if there is at least one matching packet policy cause the data processing equipment to:

determine if there is a currently active timed matching policy authorizing access to the specific website.

35. The computer program product of claim 33, wherein the user defined packet policies authorize access to specific websites by authorized users, applications, physical ports, application ports, IP addresses, or MAC addresses.

36. The computer program product of claim 33, wherein the instructions for blocking the data packet cause the data processing equipment to:

discard the data packet, log the data packet, or forward the data packet to a multilayer switch application for processing.

37. A computer program product tangibly embodied in a computer readable medium, the computer program product comprising instructions operable to cause data processing equipment to:

configure a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receive a data packet at a particular port of the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determine if there is a match between the data packet and one or more of the packet policies, each packet policy blocking matching data packets received at the particular port from utilizing the computer network;

if there is a matching packet policy blocking the data packet, block the data packet; and

if there is no matching packet policy blocking the data packet, process the data packet.

38. The computer program product of claim 37, wherein the user defined packet policies block data packets received at the particular port, for data packets having a subnet address, a range of subnet addresses, a host address, or a range of host addresses.

39. A computer program product tangibly embodied in a computer readable medium, the computer program product comprising instructions operable to cause data processing equipment to:

configure a multilayer switch to process data packets at wire-speed based on one or more user defined packet policies, each user defined packet policy specifying information for one or more of Layers 4 through 7;

receive a data packet at the multilayer switch, the data packet including information from one or more of Layers 2 through 7 of the OSI model;

determine if there is a match between the data packet and one or more of the packet policies, each packet policy specifying that surveillance is to performed on the data packet;

if there is a matching packet policy specifying surveillance, mirror the data packet to a specified location; and

process the data packet using the multilayer switch.

40. The computer program product of claim 39, wherein the instructions for processing the data packet cause the data processing equipment to:

route the data packet using a Layer 2-3 switch.